UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/511,466 | 10/15/2004 | Yuji Watanabe | JP920020083US1 | 2843 |

877 7590 08/05/2008

IBM CORPORATION, T.J. WATSON RESEARCH CENTER
P.O. BOX 218
YORKTOWN HEIGHTS, NY 10598

| EXAMINER | |
|---|---|
| CALLAHAN, PAUL E | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2137 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 08/05/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/511,466 | WATANABE ET AL. | |
| | Examiner | Art Unit | |
| | PAUL CALLAHAN | 2137 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *6-6-08*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Continued Examination Under 37 CFR 1.114*

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on June 6, 2008 has been entered.

2. Claims 1-14 are pending and have been examined.

### *Response to Arguments*

3. Applicant's arguments filed June 8, 2008 have been fully considered but they are not persuasive.

The Applicant argues that the claims as presently amended may be distinguished from the teachings of Matsuzaki. The Applicant asserts that Matsuzaki fails to teach the features of a key distribution server that distributes individual decryption information respectively corresponding to each one of said specific number of subscriber terminals and used to perform decryption of said first group key, and individual key update information respectively corresponding to each one of said specific number of subscriber terminals. However, the Examiner maintains that these steps are indeed taught at, for example, col. 13 line 52 through col. 15 line 45. The Examiner does not

agree that the added claim language clearly sets forth that the decryption information and key update information distributed to each terminal is unique to that terminal. The Examiner suggests that such a limitation if added to the claims would further distinguish them from Matsuzaki.

***Specification***

4. Claim 9 objected to because of the following informalities:

The claim is dependent on the higher numbered claim 11. Such a dependency is improper under 37 CFR 1.75(c) which requires a dependent claim to further limit a *preceding* claim. Appropriate correction is required.

***Claim Rejections - 35 USC § 101***

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 5-8 and 10-12 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

As for claims 5-7, the preambles of the claims indicate that they are directed towards an apparatus. However, all of the subsequent limitations are set forth in the form of a means for performing a particular function. As per the Applicant's Specification on page 13 lines 5 through 36, the functions set forth can be performed entirely in software. Therefore, the claims are directed towards non-statutory subject matter since

nowhere in these claims is there a limitation that sets forth the software as embodied in a computer-readable memory medium. Therefore, the claims set forth only functional descriptive language and are non-statutory since this does not fall into one of the classes of invention eligible for the grant of a US patent. Unless embodied in a computer-readable medium the software in and of itself cannot be considered as a computer component, and hence cannot effect a change of state of a processor to produce a useful or tangible result. From 2106.01: Computer-Related Nonstatutory Subject Matter: *Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, "functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component. (The definition of "data structure" is "a physical or logical relationship among data elements, designed to support specific data manipulation functions*." The New IEEE Standard Dictionary of Electrical and Electronics Terms 308 (5th ed. 1993).) *"Nonfunctional descriptive material" includes but is not limited to music, literary works, and a compilation or mere arrangement of data. Both types of "descriptive material" are nonstatutory when claimed as descriptive material per se*, 33 F.3d at 1360, 31 USPQ2d at 1759. *When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases.*

As for claims 8 and 10-12, the preamble of the claims indicate that they are directed towards "*A recording medium recording a program thereon for controlling a computer ..., said program being made readable by said computer so as to make said computer have capabilities achieved though use of said program...*". It is not explicitly clear that the recording medium is a computer-readable medium since the preamble implies that the medium is unreadable without some action taken by the computer itself. Therefore, the claims set forth only functional descriptive language and are non-statutory since this does not fall into one of the classes of invention eligible for the grant of a US patent. Unless embodied in a computer-readable medium the software in and of itself cannot be considered as a computer component, and hence cannot effect a change of state of a processor to produce a useful or tangible result. From 2106.01: Computer-Related Nonstatutory Subject Matter: *Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, "functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component. (The definition of "data structure" is "a physical or logical relationship among data elements, designed to support specific data manipulation functions*." The New IEEE Standard Dictionary of Electrical and Electronics Terms 308 (5th ed. 1993).) *"Nonfunctional descriptive material" includes but is not limited to music, literary works, and a compilation or mere arrangement of data. Both types of "descriptive material" are nonstatutory when claimed as descriptive material per se*, 33 F.3d at 1360, 31 USPQ2d

at 1759. *When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases.*

Claim 9 is dependent on claim 11 and does not cure its deficiency, therefore it is rejected on the same basis as claim 11.

***Claim Rejections - 35 USC § 102***

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1-14 are rejected under 35 U.S.C. 102(e) as being anticipated by Matsuzaki et al (US 6,813,357 B1).

As for claim 1, Matsuzaki discloses a cryptographic communication system comprising: a key distribution server for distributing a key used to decrypt encrypted information (col. 11, lines 35-47; col. 12, lines45-67; col. 13, lines 1-10); and a specific number of subscriber terminals using said information (col. 11, lines 35-47; col. 12, lines 45-47), wherein said key distribution server distributes: an encrypted first group key

used to decrypt said information (col.13, lines 30-50); individual decryption information respectively corresponding to each one of said specific number of subscriber terminals and used to perform decryption of said first group key (col. 14, lines 1-49); and individual key update information respectively corresponding to each one of said specific number of subscriber terminals and used to perform a part of decryption of a second group key, said second group key being updated after a group key is updated, and wherein said specific number of subscriber terminals decrypt said first group key distributed from said key distribution server by use of results obtained by. processing operations performed based on said key update information previously obtained and used to decrypt said first group key, as well as by use of said decryption information distributed from said key distribution server (col. 15, lines 1-44).

As for claim 2, Matsuzaki discloses the cryptographic communication system according to claim 1, wherein said specific number of subscriber terminals implement a part of decryption of said group key, said decryption being performed using said individual key update information, before distribution of said group key (col. 38, lines 1-67; coil 39, lines 1-21).

As for claim 3, Matsuzaki discloses the cryptographic communication system according to claim 1, wherein said key distribution server distributes to said specific number of subscriber terminals key update information, used to decrypt said first group

key, together with a third group key, said third group key being in a state before said third group key gets updated to said first group key (col. 31, lines 10-67; col. 32, lines 1-67).

As for claim 4, Matsuzaki discloses the cryptographic communication system according to claim 1, wherein in the event where said key distribution server updates said group key, said key distribution server determines which subscriber terminals among said specific number of subscriber terminals are to be excluded and distributes to said specific number of subscriber terminals, together with said group key being updated, said decryption information used by remaining subscriber terminals other than said subscriber terminals to be excluded to make said remaining subscriber terminals able to decrypt said group key being updated (col. 31, lines 10-67; col. 32, lines 1-67).

As for claim 5, Matsuzaki discloses a key distribution server for distributing a key used to decrypt encrypted information, comprising: means for generating a first group key used to decrypt said information and encrypting said first group key (col. 32, lines 53:62); means for generating individual decryption information used to perform decryption of said first group key and corresponding to subscriber terminals (col. 32-, lines 63-62; col. 33, lines 1-57); means for generating individual key update information used to perform a part of decryption of a second group key, said second key being updated after a group key is updated, and corresponding to said subscriber terminals (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines 1-19); and means for respectively

distributing said first group key, said decryption information and said key update information to each one of said corresponding subscriber terminals (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines 1.-19).

As for claim 6, Matsuzaki discloses the key distribution server according to claim 5, wherein said means for generating said decryption information determines which terminals among said subscriber terminals are to be excluded and generates said decryption information used by remaining subscriber terminals other than said subscriber terminals to be excluded in order to make said remaining subscriber terminals able to decrypt said group key (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines 1-19).

As for claim 7, Matsuzaki discloses a terminal device comprising: means for retrieving from a specific key distribution server a group key encrypted to decrypt encrypted information and individual decryption information corresponding to the terminal device used to decrypt said group key; means for performing a part of decryption of said group key before distribution of said group key; and means for decrypting said group key by use of results obtained by processing operations performed based on a part of decryption of said group key and said decryption information retrieved from said key distribution server (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines 1-19).

As for claim 8, Matsuzaki discloses a program for controlling a computer and then distributing a key used to decrypt encrypted information, said program making said computer have capabilities including: a function of generating a first group key used to decrypt said information and encrypting said first group key; a function of generating individual decryption information used to perform decryption of said first group key and corresponding to subscriber terminals; a function of generating individual key update information used to perform a part of decryption of a second group key, said second key being updated after a group key is updated, and corresponding to said subscriber terminals; and a function of respectively distributing said first group key, said decryption information and said key update information to each one of said corresponding subscriber terminals via specific communication means (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines. 1-19).

As for claim 9, Matsuzaki discloses the program according to claim 8, wherein said function of generating individual decryption information determines which subscriber terminals among said subscriber terminals are to be excluded and generates said decryption information used by remaining subscriber terminals other than said subscriber terminals to be excluded in order to make said remaining subscriber terminals able to decrypt said group key (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines 1-19).

As for claim 10, Matsuzaki discloses a program for controlling a computer and then achieving a specific function, said program making said computer have capabilities including: a function of retrieving from a specific key distribution server a group key encrypted to decrypt encrypted information and individual decryption information corresponding to the computer used to decrypt said group key via specific communication means; a function of performing a part of decryption of said group key before distribution of said group key; and a function of decrypting said group key by use of results obtained by processing operations performed based on a part of decryption of said group key and said decryption information retrieved from said key distribution server (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines 1-19).

As for claim 11, Matsuzaki discloses a recording medium recording a program thereon for controlling a computer and then distributing a key used to decrypt encrypted information, said program being made readable by said computer so as to make said computer have capabilities achieved though use of said program, said program including: a function of generating a first group key used to decrypt said information and encrypting said first group key; a function of generating individual decryption information used to perform decryption of said first group key and corresponding to subscriber terminals; a function of generating individual key update information used to perform a part of decryption of a second group key, said second key being updated after a group key is updated, and corresponding to said subscriber terminals; and a function of respectively distributing said first group key, said decryption

information and said key update information to each one of said corresponding subscriber terminals via specific communication means (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines 1-19).

As for claim 12, Matsuzaki discloses a recording medium recording a program thereon for controlling a computer and then achieving a specific function, said program being made readable by said computer so as to make said computer have capabilities achieved though use of said program, said program including: a function of retrieving from a specific key distribution server a group key encrypted to decrypt encrypted information and individual decryption information corresponding to the computer used to decrypt said group key via specific communication means; a function of performing a part of decryption of said group key before distribution of said group key; and a function of decrypting said group key by making use of results obtained by processing Operations performed based on a part of decryption of said group key and said decryption information retrieved from said key distribution server (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines 1-19).

As for claim 13, Matsuzaki discloses a key sharing method for making a specific number of terminals share a key used to decrypt encrypted information, said specific number of terminals making use of said information, said method comprising: a step of making said specific number of terminals perform a part of decryption of an encrypted group key used to decrypt said information before distribution of said group

key; a step of respectively distributing to said specific number of terminals said group key and individual decryption information corresponding to each one of said specific number of terminals used to perform a part of remaining decryption other than said part of decryption of said group key and .corresponding to said specific number of terminals; and a step of making said specific number of terminals perform decryption of said group key using said decryption information being distributed and results obtained by performing a part of decryption of said group key, said part of decryption previously being performed (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines 1-19).

As for claim 14, Matsuzaki discloses the key sharing method according to claim 13, wherein information used to perform said part of decryption is distributed in advance of distribution of said group key to said specific number of terminals together with said group key, said group key being in a state before being updated (col. 9, lines 30-62).

***Conclusion***

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.
If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone

number for the organization where this application or proceeding is assigned is: (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Paul Callahan/

August 1, 2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136